

On R. Chapman's "evil determinant": case $p \equiv 1 \pmod{4}$

Maxim Vsemirnov*

St. Petersburg Department of V.A.Steklov Institute of Mathematics,
27 Fontanka, St. Petersburg, 191023, Russia

and

St. Petersburg State University,
Department of Mathematics and Mechanics,
28 University prospekt, St. Petersburg, 198504, Russia
E-mail: vseмир@pdmi.ras.ru

Abstract

For $p \equiv 1 \pmod{4}$, we prove the formula (conjectured by R. Chapman) for the determinant of the $\frac{p+1}{2} \times \frac{p+1}{2}$ matrix $C = (C_{ij})$ with $C_{ij} = \left(\frac{j-i}{p}\right)$.

1 Introduction

Let p be a prime and $\left(\frac{\cdot}{p}\right)$ denote the Legendre symbol. Let us set $n = \frac{p-1}{2}$ and consider the following $(n+1) \times (n+1)$ matrix C :

$$C_{ij} = \left(\frac{j-i}{p}\right), \quad 0 \leq i, j \leq n.$$

Here and it what follows it is more natural to enumerate rows and columns starting from 0. R. Chapman [8] raised the problem of evaluating $\det C$; for motivation and related determinants see also [6], [7]. In particular, Chapman conjectured (see also [2, Problem 10]) that $\det C$ is always 1 when

*This research was supported in part by the Dynasty Foundation and RFBR (grant 09-01-00784-a) and the State Financed Task project no. 6.38.74.2011 at St. Petersburg State University.

2010 *Mathematics Subject Classification*: Primary 11C20; Secondary 11R29, 15A15, 15B05.

Key words and phrases: Legendre symbol, determinant, Cauchy determinant, Dirichlet's class number formula. .

$p \equiv 3 \pmod{4}$ and had a conjectural expression for $\det C$ in terms of the fundamental unit and class number of $\mathbb{Q}(\sqrt{p})$ for $p \equiv 1 \pmod{4}$. The sequence $\det C$ for primes $p \equiv 1 \pmod{4}$ also appears as sequence A179073 in the On-line Encyclopedia of Integer Sequences [1].

Chapman's conjecture for $p \equiv 3 \pmod{4}$ was settled affirmatively in [12]. The aim of this paper is to apply methods developed in [12] and to evaluate $\det C$ for $p \equiv 1 \pmod{4}$.

Let \mathcal{O} be the ring of integers of $\mathbb{Q}(\sqrt{p})$. Let ε be the fundamental unit in \mathcal{O} and $h = h(p)$ be the class number.

Theorem 1. *Let*

$$(1.1) \quad a + b\sqrt{p} = \begin{cases} \varepsilon^h, & \text{if } p \equiv 1 \pmod{8}, \\ \varepsilon^{3h}, & \text{if } p \equiv 5 \pmod{8}, \end{cases}$$

Then $\det C = -a$.

Our proof is divided into three steps. First, we decompose C into a product of several matrices; see Theorem 2 below. This part resembles a similar step in the evaluation of $\det C$ for $p \equiv 3 \pmod{4}$; see [12] for details. Second, we find general expressions for certain parametric Cauchy-type determinants and reduce our problem to a particular case of that calculation. Finally, we relate the obtained determinants to Dirichlet's class number formula for real quadratic fields [4, Ch. 5, §4], which involves both class number and the fundamental unit.

Looking at the numerical data, W. Zudilin and J. Sondow conjectured [1, Entry A179073] that $\det C$ is always negative and even. This easily follows from our Theorem 1.

Corollary 1. *For $p \equiv 1 \pmod{4}$, $\det C$ is negative and even.*

2 Matrix decomposition

Set $n = (p-1)/2$. Let ζ be the primitive p -th root of unity with $\arg \zeta = 2\pi/p$. We also fix its square root $\zeta^{1/2}$ such that $\arg \zeta^{1/2} = \pi/p$.

Let us consider the following three matrices U , V , and D :

$$(2.1) \quad U_{ij} = \frac{\binom{i}{p} \zeta^{-j-2i} + \binom{j}{p} \zeta^{-2j-i}}{\zeta^{-i-j} + \binom{i}{p} \binom{j}{p}}, \quad 0 \leq i, j \leq n,$$

$$V_{ij} = \zeta^{2ij}, \quad 0 \leq i, j \leq n,$$

$$(2.2) \quad D_{ii} = \prod_{\substack{0 \leq k \leq n \\ k \neq i}} \frac{1}{\zeta^{2i} - \zeta^{2k}}, \quad 0 \leq i \leq n,$$

$$(2.3) \quad D_{ij} = 0, \quad i \neq j.$$

In particular, V is a Vandermonde-type matrix and D is diagonal. If we set

$$g(x) = \prod_{0 \leq k \leq n} (x - \zeta^{2k}),$$

then the diagonal entries of D can be represented in an alternative way as

$$(2.4) \quad D_{ii} = \frac{1}{g'(\zeta^{2i})}.$$

Finally, let $\tau_p(r)$ be the Gauss sum

$$\tau_p(r) = \sum_{k=1}^{p-1} \left(\frac{kr}{p} \right) \zeta^k = \sum_{k=1}^{p-1} \left(\frac{k}{p} \right) \zeta^{kr}.$$

Theorem 2. *For any prime p such that $p \equiv 1 \pmod{4}$, we have*

$$(2.5) \quad C = \tau_p(2) \zeta^{(p-1)/4} \cdot V D U D V = \left(\frac{2}{p} \right) \sqrt{p} \zeta^{(p-1)/4} \cdot V D U D V.$$

Remark 1. For $p \equiv 3 \pmod{4}$ we have (see [12]) a similar expression

$$C = -\tau_p(2) \zeta^{-(p+1)/4} \cdot V D \tilde{U} D V,$$

where

$$(2.6) \quad \tilde{U}_{ij} = \frac{\left(\frac{i}{p} \right) \zeta^{-j-2i} - \left(\frac{j}{p} \right) \zeta^{-2j-i}}{\zeta^{-i-j} - \left(\frac{i}{p} \right) \left(\frac{j}{p} \right)}.$$

Both (2.1) for $p \equiv 1 \pmod{4}$ and (2.6) for $p \equiv 3 \pmod{4}$ can be unified as

$$U_{ij} = \frac{\left(\frac{i}{p} \right) \zeta^{-j-2i} + \left(\frac{-j}{p} \right) \zeta^{-2j-i}}{\zeta^{-i-j} + \left(\frac{i}{p} \right) \left(\frac{-j}{p} \right)}.$$

The unified formula for the decomposition becomes $C = \left(\frac{-1}{p} \right) \tau_p(2) \zeta^{(p^2-1)/4} \cdot V D U D V$.

Proof of Theorem 2. Let $B = V D U D V$. We have,

$$B_{ij} = \sum_{k=0}^n \sum_{r=0}^n \zeta^{2ki+2rj} \cdot \frac{1}{g'(\zeta^{2k})} \cdot \frac{1}{g'(\zeta^{2r})} \cdot \frac{\left(\frac{k}{p} \right) \zeta^{-r-2k} + \left(\frac{r}{p} \right) \zeta^{-2r-k}}{\zeta^{-k-r} + \left(\frac{k}{p} \right) \left(\frac{r}{p} \right)}.$$

The term corresponding to $k = r = 0$ in the above sum vanishes. The remaining terms can be arranged into three groups depending on whether $k = 0$, or $r = 0$, or $k \neq 0, r \neq 0$. More precisely,

$$B_{ij} = s_0 + s_1 + s_2,$$

where

$$\begin{aligned} s_0 &= \frac{1}{g'(1)} \sum_{r=1}^n \left(\frac{r}{p}\right) \cdot \frac{\zeta^{(2j-1)r}}{g'(\zeta^{2r})}, \\ s_1 &= \frac{1}{g'(1)} \sum_{k=1}^n \left(\frac{k}{p}\right) \cdot \frac{\zeta^{(2i-1)k}}{g'(\zeta^{2k})}, \\ s_2 &= \sum_{k=1}^n \sum_{r=1}^n \zeta^{2ki+2rj} \cdot \frac{1}{g'(\zeta^{2k})} \cdot \frac{1}{g'(\zeta^{2r})} \cdot \frac{\left(\frac{k}{p}\right)\zeta^{-r-2k} + \left(\frac{r}{p}\right)\zeta^{-2r-k}}{\zeta^{-k-r} + \left(\frac{k}{p}\right)\left(\frac{r}{p}\right)}. \end{aligned}$$

Notice that $\zeta^{-2k-2r} \neq 1$ and $\left(\left(\frac{k}{p}\right)\left(\frac{r}{p}\right)\right)^2 = 1$ for $1 \leq k, r \leq n$. Applying the identity

$$\left(\zeta^a - \left(\frac{k}{p}\right)\left(\frac{r}{p}\right)\right) \left(\zeta^a + \left(\frac{k}{p}\right)\left(\frac{r}{p}\right)\right) = \zeta^{2a} - 1,$$

which is valid for k, r such that $p \nmid k, p \nmid r$, we have that

$$\begin{aligned} s_2 &= \sum_{k=1}^n \sum_{r=1}^n \frac{\zeta^{2ki+2rj}}{g'(\zeta^{2k})g'(\zeta^{2r})} \cdot \frac{\left(\zeta^{-k-r} - \left(\frac{k}{p}\right)\left(\frac{r}{p}\right)\right) \left(\left(\frac{k}{p}\right)\zeta^{-r-2k} + \left(\frac{r}{p}\right)\zeta^{-2r-k}\right)}{\zeta^{-2k-2r} - 1} \\ &= \sum_{k=1}^n \sum_{r=1}^n \frac{\zeta^{2ki+2rj}}{g'(\zeta^{2k})g'(\zeta^{2r})} \cdot \frac{\left(\frac{k}{p}\right)(\zeta^{-2r-3k} - \zeta^{-2r-k}) + \left(\frac{r}{p}\right)(\zeta^{-3r-2k} - \zeta^{-r-2k})}{\zeta^{-2k-2r} - 1} \\ &= s_3 + s_4, \end{aligned}$$

where

$$\begin{aligned} s_3 &= \sum_{k=1}^n \sum_{r=1}^n \left(\frac{k}{p}\right) \frac{\zeta^{2ki+2rj}}{g'(\zeta^{2k})g'(\zeta^{2r})} \cdot \frac{\zeta^{-2r-3k} - \zeta^{-2r-k}}{\zeta^{-2k-2r} - 1} \\ &= \sum_{k=1}^n \sum_{r=1}^n \left(\frac{k}{p}\right) \frac{\zeta^{2ki+2rj}}{g'(\zeta^{2k})g'(\zeta^{2r})} \cdot \frac{\zeta^{-3k} - \zeta^{-k}}{\zeta^{-2k} - \zeta^{2r}}, \\ s_4 &= \sum_{k=1}^n \sum_{r=1}^n \left(\frac{r}{p}\right) \frac{\zeta^{2ki+2rj}}{g'(\zeta^{2k})g'(\zeta^{2r})} \cdot \frac{\zeta^{-3r-2k} - \zeta^{-r-2k}}{\zeta^{-2k-2r} - 1} \\ &= \sum_{k=1}^n \sum_{r=1}^n \left(\frac{r}{p}\right) \frac{\zeta^{2ki+2rj}}{g'(\zeta^{2k})g'(\zeta^{2r})} \cdot \frac{\zeta^{-3r} - \zeta^{-r}}{\zeta^{-2r} - \zeta^{2k}}. \end{aligned}$$

By the Lagrange interpolation formula, for any polynomial f of degree less than $n+1$, we have that

$$\frac{f(x)}{g(x)} = \sum_{r=0}^n \frac{1}{g'(\zeta^{2r})} \cdot \frac{f(\zeta^{2r})}{x - \zeta^{2r}}.$$

Therefore, for any x different from the roots of g ,

$$(2.7) \quad \sum_{r=1}^n \frac{1}{g'(\zeta^{2r})} \cdot \frac{f(\zeta^{2r})}{x - \zeta^{2r}} = \frac{f(x)}{g(x)} - \frac{1}{g'(1)} \cdot \frac{f(1)}{x - 1}.$$

If k runs through $1, \dots, n$, then $-2k \pmod{p}$ runs through odd integers $p-2, p-4, \dots, 3, 1$. In particular, ζ^{-2k} is not a root of g . To evaluate s_3 we make summation with respect to r first and use (2.7) for $f(x) = x^j$ substituting $x = \zeta^{-2k}$:

$$\begin{aligned}
s_3 &= \sum_{k=1}^n \left(\frac{k}{p}\right) \frac{\zeta^{2ki}}{g'(\zeta^{2k})} (\zeta^{-3k} - \zeta^{-k}) \left(\sum_{r=1}^n \frac{1}{g'(\zeta^{2r})} \cdot \frac{\zeta^{2rj}}{\zeta^{-2k} - \zeta^{2r}} \right) \\
&= \sum_{k=1}^n \left(\frac{k}{p}\right) \frac{\zeta^{2ki}}{g'(\zeta^{2k})} (\zeta^{-3k} - \zeta^{-k}) \left(\frac{\zeta^{-2kj}}{g(\zeta^{-2k})} - \frac{1}{g'(1)} \cdot \frac{1}{\zeta^{-2k} - 1} \right) \\
&= \sum_{k=1}^n \left(\frac{k}{p}\right) \frac{\zeta^{2k(i-j)}(\zeta^{-3k} - \zeta^{-k})}{g'(\zeta^{2k})g(\zeta^{-2k})} - \frac{1}{g'(1)} \sum_{k=1}^n \left(\frac{k}{p}\right) \frac{\zeta^{(2i-1)k}}{g'(\zeta^{2k})} \\
&= \sum_{k=1}^n \left(\frac{k}{p}\right) \frac{\zeta^{2k(i-j)}(\zeta^{-3k} - \zeta^{-k})}{g'(\zeta^{2k})g(\zeta^{-2k})} - s_1.
\end{aligned}$$

To evaluate s_4 we argue in the same way but now we sum with respect to k first and substitute $x = \zeta^{-2r}$ into (2.7) for $f(x) = x^i$. As a result,

$$s_4 = \sum_{r=1}^n \left(\frac{r}{p}\right) \frac{\zeta^{2r(j-i)}(\zeta^{-3r} - \zeta^{-r})}{g'(\zeta^{2r})g(\zeta^{-2r})} - s_0.$$

Therefore,

$$\begin{aligned}
B_{ij} &= \sum_{k=1}^n \left(\frac{k}{p}\right) \frac{\zeta^{2k(i-j)}(\zeta^{-3k} - \zeta^{-k})}{g'(\zeta^{2k})g(\zeta^{-2k})} + \sum_{r=1}^n \left(\frac{r}{p}\right) \frac{\zeta^{2r(j-i)}(\zeta^{-3r} - \zeta^{-r})}{g'(\zeta^{2r})g(\zeta^{-2r})} \\
&= \sum_{k=1}^n \left(\frac{k}{p}\right) \frac{(\zeta^{2k(i-j)} + \zeta^{-2k(i-j)})(\zeta^{-3k} - \zeta^{-k})}{g'(\zeta^{2k})g(\zeta^{-2k})}.
\end{aligned}$$

Now we evaluate the denominator of each term. Recall that $n = (p-1)/2$, so $(-1)^{n+1} = (-1)^{(p+1)/2} = -1$ if $p \equiv 1 \pmod{4}$. We have

$$\begin{aligned}
g'(\zeta^{2k})g(\zeta^{-2k}) &= \prod_{\substack{0 \leq t \leq n \\ t \neq k}} (\zeta^{2k} - \zeta^{2t}) \prod_{0 \leq t \leq n} (\zeta^{-2k} - \zeta^{2t}) \\
&= (-1)^{n+1} (\zeta^{-2k})^{n+1} (\zeta^2)^{(0+1+\dots+n)} \prod_{\substack{0 \leq t \leq n \\ t \neq k}} (\zeta^{2k} - \zeta^{2t}) \prod_{0 \leq t \leq n} (\zeta^{2k} - \zeta^{-2t}) \\
&= -\zeta^{-k(p+1)} \zeta^{(p^2-1)/4} (\zeta^{2k} - 1) \prod_{\substack{0 \leq t \leq p-1 \\ t \neq k}} (\zeta^{2k} - \zeta^{2t}) \\
&= -\zeta^{-k} \zeta^{(p-1)/4} (\zeta^{2k} - 1) ((x^p - 1)')|_{x=\zeta^{2k}} \\
&= -p \zeta^{-3k} \zeta^{(p-1)/4} (\zeta^{2k} - 1).
\end{aligned}$$

Using this together with the fact that $\left(\frac{\cdot}{p}\right)$ is an even character for $p \equiv 1$

(mod 4), we continue as follows:

$$\begin{aligned}
B_{ij} &= \frac{\zeta^{-(p-1)/4}}{p} \sum_{k=1}^n \left(\frac{k}{p}\right) (\zeta^{2k(i-j)} + \zeta^{-2k(i-j)}) \\
&= \frac{\zeta^{-(p-1)/4}}{p} \sum_{k=1}^n \left(\left(\frac{k}{p}\right) \zeta^{2k(i-j)} + \left(\frac{-k}{p}\right) \zeta^{-2k(i-j)} \right) \\
&= \frac{\zeta^{-(p-1)/4}}{p} \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \zeta^{2k(i-j)} \\
&= \left(\frac{i-j}{p}\right) \frac{\zeta^{-(p-1)/4}}{p} \sum_{r=1}^{p-1} \left(\frac{r}{p}\right) \zeta^{2r} = \left(\frac{j-i}{p}\right) \frac{\zeta^{-(p-1)/4} \tau_p(2)}{p}.
\end{aligned}$$

Since $\tau_p(2) = \left(\frac{2}{p}\right) \sqrt{p}$ for $p \equiv 1 \pmod{4}$ (e.g., see [9, Ch. 6]), we conclude that

$$\zeta^{(p-1)/4} \tau_p(2) B_{ij} = \left(\frac{2}{p}\right) \sqrt{p} \zeta^{(p-1)/4} B_{ij} = \left(\frac{j-i}{p}\right) = C_{ij},$$

which completes the proof. \square

3 Determinants of Cauchy-like matrices

The following identity is due to Cauchy [5]:

$$\det \left(\frac{1}{u_i + v_j} \right)_{i,j=0,\dots,m-1} = \prod_{0 \leq i < j \leq m-1} ((u_i - u_j)(v_i - v_j)) \prod_{0 \leq i, j \leq m-1} (u_i + v_j)^{-1}.$$

An alternative form of this identity can be obtained by replacing v_j with v_j^{-1} and multiplying each column by v_j^{-1} :

$$\begin{aligned}
(3.1) \quad \det \left(\frac{1}{1 + u_i v_j} \right)_{i,j=0,\dots,m-1} \\
= \prod_{0 \leq i < j \leq m-1} ((u_i - u_j)(v_j - v_i)) \prod_{0 \leq i, j \leq m-1} (1 + u_i v_j)^{-1}.
\end{aligned}$$

For further connections of (3.1) with representation theory and symmetric functions, see [11, Ch. 7].

In this section we evaluate determinants of several parametric matrices related to the second form of the Cauchy identity. Let $\vec{u} = (u_0, \dots, u_{m-1})$, $\vec{v} = (v_0, \dots, v_{m-1})$. Assume further that $1 + u_i v_j \neq 0$, $i, j = 0, \dots, m-1$. Let $M_m(\vec{u}, \vec{v})$ be the $m \times m$ matrix with

$$(M_m(\vec{u}, \vec{v}))_{ij} = \frac{u_i + v_j}{1 + u_i v_j}.$$

Theorem 3. We have¹ $\det M_m(\vec{u}, \vec{v}) =$

$$\begin{aligned} &= \frac{1}{2} \left(\prod_{i=0}^{m-1} (1 + u_i) \prod_{j=0}^{m-1} (1 + v_j) + (-1)^m \prod_{i=0}^{m-1} (1 - u_i) \prod_{j=0}^{m-1} (1 - v_j) \right) \\ &\quad \times \prod_{0 \leq i < j \leq m-1} (u_i - u_j) \prod_{0 \leq i < j \leq m-1} (v_j - v_i) \prod_{i=0}^{m-1} \prod_{j=0}^{m-1} (1 + u_i v_j)^{-1}. \end{aligned}$$

Proof. Let J be the $m \times m$ matrix with all entries equal to 1. Consider

$$f(t) = \det(tJ + M_m(\vec{u}, \vec{v})).$$

Since J has rank 1, there are two invertible matrices H_1 and H_2 with coefficients independent of the variable t , such that

$$H_1 J H_2 = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix}.$$

Since $f(t) = \det H_1^{-1} \det(tH_1 J H_2 + H_1 M_m(\vec{u}, \vec{v}) H_2) \det H_2^{-1}$, the function f is linear with respect to t . In particular, $\det M_m(\vec{u}, \vec{v}) = f(0) = (f(1) + f(-1))/2$. On the other hand,

$$\begin{aligned} f(1) &= \det \left(1 + \frac{u_i + v_j}{1 + u_i v_j} \right)_{i,j=0,\dots,m-1} = \det \left(\frac{(1 + u_i)(1 + v_j)}{1 + u_i v_j} \right)_{i,j=0,\dots,m-1} \\ &= \prod_{i=0}^{m-1} (1 + u_i) \prod_{j=0}^{m-1} (1 + v_j) \cdot \det \left(\frac{1}{1 + u_i v_j} \right)_{i,j=0,\dots,m-1}, \end{aligned}$$

In a similar way

$$\begin{aligned} f(-1) &= \det \left(-1 + \frac{u_i + v_j}{1 + u_i v_j} \right)_{i,j=0,\dots,m-1} \\ &= \det \left(\frac{-(1 - u_i)(1 - v_j)}{1 + u_i v_j} \right)_{i,j=0,\dots,m-1} \\ &= (-1)^m \prod_{i=0}^{m-1} (1 - u_i) \prod_{j=0}^{m-1} (1 - v_j) \cdot \det \left(\frac{1}{1 + u_i v_j} \right)_{i,j=0,\dots,m-1}. \end{aligned}$$

Combining this with (3.1) we complete the proof. \square

¹When the paper was ready, T. Amdeberhan informed the author that an equivalent statement had been proved in [3] by a different method.

Now let $\vec{x} = (x_1, \dots, x_m)$, $\vec{y} = (y_1, \dots, y_m)$ and assume that $1 + x_i y_j \neq 0$, $1 + x_i \neq 0$, $1 + y_j \neq 0$, $i, j = 1, \dots, m$. Let $W_m(\vec{x}, \vec{y})$ be the following $(m+1) \times (m+1)$ matrix:

$$W_m(\vec{x}, \vec{y}) = \left(\begin{array}{c|ccc} 0 & 1 & \dots & 1 \\ \hline 1 & & & \\ \vdots & & & \\ 1 & & & \end{array} \begin{array}{c} M_m(\vec{x}, \vec{y}) \end{array} \right).$$

Theorem 4. We have $\det W_m(\vec{x}, \vec{y}) =$

$$\begin{aligned} &= -\frac{1}{2} \left(\prod_{i=1}^m (1 + x_i) \prod_{j=1}^m (1 + y_j) - (-1)^m \prod_{i=1}^m (1 - x_i) \prod_{j=1}^m (1 - y_j) \right) \\ &\quad \times \prod_{1 \leq i < j \leq m} (x_i - x_j) \prod_{1 \leq i < j \leq m} (y_j - y_i) \prod_{i=1}^m \prod_{j=1}^m (1 + x_i y_j)^{-1}. \end{aligned}$$

Proof. Since

$$M_{m+1}((1, \vec{x}), (1, \vec{y})) = \left(\begin{array}{c|ccc} 1 & 1 & \dots & 1 \\ \hline 1 & & & \\ \vdots & & & \\ 1 & & & \end{array} \begin{array}{c} M_m(\vec{x}, \vec{y}) \end{array} \right),$$

we have that

$$\begin{aligned} (3.2) \quad \det W_m(\vec{x}, \vec{y}) &= \det M_{m+1}((1, \vec{x}), (1, \vec{y})) - \det \left(\begin{array}{c|ccc} 1 & 0 & \dots & 0 \\ \hline 1 & & & \\ \vdots & & & \\ 1 & & & \end{array} \begin{array}{c} M_m(\vec{x}, \vec{y}) \end{array} \right) \\ &= \det M_{m+1}((1, \vec{x}), (1, \vec{y})) - \det M_m(\vec{x}, \vec{y}). \end{aligned}$$

By Theorem 3,

$$\begin{aligned} \det M_{m+1}((1, \vec{x}), (1, \vec{y})) &= \frac{(1+1)(1+1)}{2(1+1)} \prod_{i=1}^m (1 + x_i) \prod_{j=1}^m (1 + y_j) \\ &\quad \times \prod_{j=1}^m (1 - x_j) \prod_{1 \leq i < j \leq m} (x_i - x_j) \prod_{j=1}^m (y_j - 1) \prod_{1 \leq i < j \leq m} (y_j - y_i) \\ &\quad \times \prod_{j=1}^m (1 + y_j)^{-1} \prod_{i=1}^m (1 + x_i)^{-1} \prod_{i=1}^m \prod_{j=1}^m (1 + x_i y_j)^{-1} + 0 \\ &= (-1)^m \prod_{i=1}^m (1 - x_i) \prod_{j=1}^m (1 - y_j) \prod_{1 \leq i < j \leq m} (x_i - x_j) \prod_{1 \leq i < j \leq m} (y_j - y_i) \\ &\quad \times \prod_{i=1}^m \prod_{j=1}^m (1 + x_i y_j)^{-1}. \end{aligned}$$

Applying Theorem 3 to the evaluation of $\det M_m(\vec{x}, \vec{y})$ and using (3.2) we complete the proof. \square

4 Evaluation of the determinant

Recall that $n = (p - 1)/2$. Let G be the diagonal matrix with

$$(4.1) \quad G_{00} = 1, \quad G_{ii} = \left(\frac{i}{p}\right) \zeta^i, \quad i = 1, \dots, n.$$

Set

$$(4.2) \quad W = GUG.$$

By a direct computation, $W_{00} = 0$,

$$\begin{aligned} W_{0j} &= W_{j0} = 1, \quad j = 1, \dots, n, \\ W_{ij} &= \frac{\left(\frac{i}{p}\right) \zeta^i + \left(\frac{j}{p}\right) \zeta^j}{1 + \left(\frac{i}{p}\right) \left(\frac{j}{p}\right) \zeta^{i+j}}, \quad i, j = 1, \dots, n. \end{aligned}$$

In particular, $W = W_n(\vec{x}, \vec{y})$, where $x_i = y_i = \left(\frac{i}{p}\right) \zeta^i$, $i = 1, \dots, n$. Now we apply Theorem 4. The last product in the expression for $\det W_n$ can be transformed in the following way: first we extract terms with $i = j$ and then we join together the two factors corresponding to (i, j) and (j, i) for $i \neq j$. Taking into account that $(-1)^n = (-1)^{(p-1)/2} = 1$ for $p \equiv 1 \pmod{4}$, we conclude that

$$(4.3) \quad \det W = -\frac{(-1)^{n(n-1)/2}}{2} \left(\prod_{j=1}^n \left(1 + \left(\frac{j}{p}\right) \zeta^j\right)^2 - \prod_{j=1}^n \left(1 - \left(\frac{j}{p}\right) \zeta^j\right)^2 \right) \\ \times \prod_{1 \leq i < j \leq n} \left(\left(\frac{i}{p}\right) \zeta^i - \left(\frac{j}{p}\right) \zeta^j \right)^2 \prod_{1 \leq i < j \leq n} \left(1 + \left(\frac{i}{p}\right) \left(\frac{j}{p}\right) \zeta^{i+j}\right)^{-2} \prod_{j=1}^n (1 + \zeta^{2j})^{-1}.$$

The following auxiliary result is an easy consequence of standard methods of evaluating Gauss sums. We present its proof for the sake of completeness.

Lemma 1. *If $p \nmid r$, then*

$$(4.4) \quad \prod_{j=1}^n (\zeta^{2rj} - \zeta^{-2rj}) = \left(\frac{r}{p}\right) \sqrt{p}.$$

Proof. By [9, Proposition 6.4.3],

$$\begin{aligned} \sqrt{p} &= \prod_{k=1}^n (\zeta^{2k-1} - \zeta^{-(2k-1)}) = (-1)^n \prod_{k=1}^n (\zeta^{p-(2k-1)} - \zeta^{-p+(2k-1)}) \\ &= \prod_{j=1}^n (\zeta^{2j} - \zeta^{-2j}). \end{aligned}$$

Let us apply the automorphism γ of $\mathbb{Q}(\zeta)$ induced by $\gamma(\zeta) = \zeta^r$. It follows from the standard properties of Gauss sums that $\gamma(\sqrt{p}) = \left(\frac{r}{p}\right)\sqrt{p}$, which completes the proof. \square

Corollary 2. *We have*

$$(4.5) \quad \prod_{j=1}^n (\zeta^{j/2} - \zeta^{-j/2}) = \left(\frac{2}{p}\right) \sqrt{p} = (-1)^{n/2} \sqrt{p},$$

$$(4.6) \quad \prod_{j=1}^n (1 + \zeta^{2j}) = \zeta^{n(n+1)/2} \left(\frac{2}{p}\right).$$

Proof. We have $\zeta^{1/2} = -\zeta^{(p+1)/2}$. Hence,

$$\begin{aligned} \prod_{j=1}^n (\zeta^{j/2} - \zeta^{-j/2}) &= \prod_{j=1}^n ((-\zeta^{(p+1)/2})^j - (-\zeta^{(p+1)/2})^{-j}) \\ &= (-1)^{n/2} \prod_{j=1}^n ((\zeta^{(p+1)/2})^j - (\zeta^{(p+1)/2})^{-j}). \end{aligned}$$

(Here we extract -1 from each term that corresponds to an odd j .) The first desired identity now follows from Lemma 1 applied to $r = (1-p)/4$ and from the fact that, for $p \equiv 1 \pmod{4}$, $(-1)^{n/2} = (-1)^{(p-1)/4} = \left(\frac{2}{p}\right)$. To prove the second identity we use the equality $1 + \zeta^{2j} = \zeta^j(\zeta^{2j} - \zeta^{-2j})(\zeta^j - \zeta^{-j})^{-1}$ and Lemma 1 applied to $r = 1$ and $r = (p+1)/2$. \square

Lemma 2. *We have*

$$\frac{1}{2} \left(\prod_{j=1}^n \left(1 + \left(\frac{j}{p}\right) \zeta^j \right)^2 - \prod_{j=1}^n \left(1 - \left(\frac{j}{p}\right) \zeta^j \right)^2 \right) = (-1)^{n/2} \zeta^{n(n+1)/2} a \sqrt{p},$$

where a is defined in (1.1).

Proof. Let

$$s = \prod_{j=1}^n \left(1 + \left(\frac{j}{p}\right) \zeta^j \right)^2.$$

Notice that $(1 + \left(\frac{j}{p}\right) \zeta^j)^2 = (\zeta^j + \left(\frac{j}{p}\right))^2$. We have

$$\begin{aligned} s &= \prod_{j=1}^n \left(\zeta^j + \left(\frac{j}{p}\right) \right)^2 = \zeta^{n(n+1)/2} \prod_{j=1}^n \left(\zeta^{j/2} + \left(\frac{j}{p}\right) \zeta^{-j/2} \right)^2 \\ &= \zeta^{n(n+1)/2} \prod_{\substack{1 \leq j \leq n \\ (j/p)=-1}} (\zeta^{j/2} - \zeta^{-j/2})^2 \prod_{\substack{1 \leq j \leq n \\ (j/p)=1}} (\zeta^{j/2} + \zeta^{-j/2})^2 \\ &= \zeta^{n(n+1)/2} \prod_{\substack{1 \leq j \leq n \\ (j/p)=-1}} (\zeta^{j/2} - \zeta^{-j/2})^2 \prod_{\substack{1 \leq j \leq n \\ (j/p)=1}} (\zeta^{j/2} - \zeta^{-j/2})^{-2} \\ &\quad \times \prod_{\substack{1 \leq j \leq n \\ (j/p)=1}} (\zeta^j - \zeta^{-j})^2 \prod_{j=1}^n (\zeta^{j/2} - \zeta^{-j/2})^{-1} \prod_{j=1}^n (\zeta^{j/2} - \zeta^{-j/2}). \end{aligned}$$

Since $\left(\frac{\cdot}{p}\right)$ is an even character for $p \equiv 1 \pmod{4}$, the number of quadratic residues modulo p on the interval $[1, n]$ equals the number of quadratic non-residues on the same interval. Therefore, we can continue as follows

$$\begin{aligned} s &= \zeta^{n(n+1)/2} \prod_{\substack{1 \leq j \leq n \\ (j/p) = -1}} \left(\sin \frac{\pi j}{p}\right)^2 \prod_{\substack{1 \leq j \leq n \\ (j/p) = 1}} \left(\sin \frac{\pi j}{p}\right)^{-2} \prod_{\substack{1 \leq j \leq n \\ (j/p) = 1}} \left(\sin \frac{2\pi j}{p}\right)^2 \\ &\quad \times \prod_{j=1}^n \left(\sin \frac{\pi j}{p}\right)^{-1} \prod_{j=1}^n (\zeta^{j/2} - \zeta^{-j/2}). \end{aligned}$$

Let us consider the third and the fourth products more carefully. We have $\sin(2\pi j/p) = \sin(\pi(p-2j)/p)$. Moreover, the map $j \mapsto p-2j$ gives a bijection between the sets

$$\{j : n/2 < j \leq n, \left(\frac{j}{p}\right) = 1\} \text{ and } \{k : 1 \leq k \leq n, k \text{ is odd}, \left(\frac{k}{p}\right) = \left(\frac{2}{p}\right)\},$$

while the map $j \mapsto 2j$ is the bijection between

$$\{j : 1 \leq j \leq n/2, \left(\frac{j}{p}\right) = 1\} \text{ and } \{k : 1 \leq k \leq n, k \text{ is even}, \left(\frac{k}{p}\right) = \left(\frac{2}{p}\right)\}.$$

Therefore,

$$\prod_{\substack{1 \leq j \leq n \\ (j/p) = 1}} \left(\sin \frac{2\pi j}{p}\right)^2 \prod_{j=1}^n \left(\sin \frac{\pi j}{p}\right)^{-1} = \prod_{\substack{1 \leq k \leq n \\ (k/p) = (2/p)}} \sin \frac{\pi k}{p} \prod_{\substack{1 \leq k \leq n \\ (k/p) = -(2/p)}} \left(\sin \frac{\pi k}{p}\right)^{-1}.$$

By Dirichet's class number formula for real quadratic fields (e.g., see [4, Ch. 5, §4]),

$$\varepsilon^h = \prod_{\substack{1 \leq j \leq n \\ (j/p) = -1}} \sin \frac{\pi j}{p} \prod_{\substack{1 \leq j \leq n \\ (j/p) = 1}} \left(\sin \frac{\pi j}{p}\right)^{-1}.$$

Combining with the above equalities, we conclude that

$$(4.7) \quad \prod_{j=1}^n \left(1 + \left(\frac{j}{p}\right) \zeta^j\right)^2 = \zeta^{n(n+1)/2} \varepsilon^{(2-(2/p))h} \prod_{j=1}^n (\zeta^{j/2} - \zeta^{-j/2}).$$

In a similar way,

$$(4.8) \quad \prod_{j=1}^n \left(1 - \left(\frac{j}{p}\right) \zeta^j\right)^2 = \zeta^{n(n+1)/2} \varepsilon^{-(2-(2/p))h} \prod_{j=1}^n (\zeta^{j/2} - \zeta^{-j/2}).$$

It is well known that ε^h is a quadratic unit of norm -1 (which is equivalent to the fact that the norm of ε is -1 and h is odd); e.g. see [10, Ch. 4, §18.4] or [4, Ch. 5, Sec. 4, Ex. 5]. It follows that

$$(4.9) \quad \varepsilon^{(2-(2/p))h} - \varepsilon^{-(2-(2/p))h} = 2a,$$

where a is defined in (1.1).

Applying Corollary 2 to the evaluation of $\prod_{j=1}^n (\zeta^{j/2} - \zeta^{-j/2})$ we complete the proof. \square

Proof of Theorem 1. It follows from Theorem 2, Lemma 2 and equations (4.2), (4.3), (4.6) that

$$(4.10) \quad \det C = -\zeta^{(n+1)(p-1)/4} \left(\left(\frac{2}{p} \right) \sqrt{p} \right)^{n+2} \times (\det V)^2 (\det D)^2 (\det G)^{-2} f_1^2 f_2^{-2} a,$$

where

$$f_1 = \prod_{1 \leq i < j \leq n} \left(\left(\frac{i}{p} \right) \zeta^i - \left(\frac{j}{p} \right) \zeta^j \right),$$

$$f_2 = \prod_{1 \leq i < j \leq n} \left(1 + \left(\frac{i}{p} \right) \left(\frac{j}{p} \right) \zeta^{i+j} \right)$$

and a is defined by (1.1). Clearly, $\det G \in (\mathbb{Z}[\zeta])^*$ by (4.1).

Let us recall some well-known facts about the arithmetic of the ring $\mathbb{Z}[\zeta]$. The reader may find further details in [9, Ch. 13]. The ideal $(1 - \zeta)$ is prime in $\mathbb{Z}[\zeta]$ and $p = \alpha(1 - \zeta)^{p-1}$, where α is a unit in $\mathbb{Z}[\zeta]$. In particular, $\sqrt{p} = \tau_p(1) = \alpha_1(1 - \zeta)^n$, where $\alpha_1 \in (\mathbb{Z}[\zeta])^*$. Finally, $(1 - \zeta^c)/(1 - \zeta)$ and $1 + \zeta^c$ are in $(\mathbb{Z}[\zeta])^*$ provided $p \nmid c$.

Notice that

$$\det V = \prod_{0 \leq i < j \leq n} (\zeta^{2j} - \zeta^{2i})$$

by the well-known evaluation of the Vandermonde determinant. Using this together with the definition of D (see (2.2), (2.3)) and the above observations we find that

$$(\sqrt{p})^{n+1} (\det V)^2 (\det D)^2 \in (\mathbb{Z}[\zeta])^*.$$

Since $\left(\frac{\cdot}{p} \right)$ is an even character and $n = (p-1)/2$, there are $n/2$ quadratic residues and $n/2$ quadratic non-residues modulo p on the interval $[1, n]$. Thus,

$$\#\{(i, j) : 1 \leq i, j \leq n, \left(\frac{i}{p} \right) = \left(\frac{j}{p} \right)\} = n^2/2,$$

$$\#\{(i, j) : 1 \leq i, j \leq n, \left(\frac{i}{p} \right) = -\left(\frac{j}{p} \right)\} = n^2/2.$$

Since the pairs (i, i) are in the first set and the pairs (i, j) and (j, i) are in one and the same set,

$$\#\{(i, j) : 1 \leq i < j \leq n, \left(\frac{i}{p} \right) = \left(\frac{j}{p} \right)\} = n(n-2)/4,$$

$$\#\{(i, j) : 1 \leq i < j \leq n, \left(\frac{i}{p} \right) = -\left(\frac{j}{p} \right)\} = n^2/4.$$

In addition,

$$\left(\frac{i}{p} \right) \zeta^i - \left(\frac{j}{p} \right) \zeta^j \in \begin{cases} (\mathbb{Z}[\zeta])^*, & \text{if } \left(\frac{i}{p} \right) \neq \left(\frac{j}{p} \right), \\ (1 - \zeta)(\mathbb{Z}[\zeta])^*, & \text{if } \left(\frac{i}{p} \right) = \left(\frac{j}{p} \right), \end{cases}$$

$$1 + \left(\frac{i}{p} \right) \left(\frac{j}{p} \right) \zeta^{i+j} \in \begin{cases} (\mathbb{Z}[\zeta])^*, & \text{if } \left(\frac{i}{p} \right) = \left(\frac{j}{p} \right), \\ (1 - \zeta)(\mathbb{Z}[\zeta])^*, & \text{if } \left(\frac{i}{p} \right) \neq \left(\frac{j}{p} \right). \end{cases}$$

Therefore, $\sqrt{p}f_1^2f_2^{-2} \in (\mathbb{Z}[\zeta])^*$.

Finally, notice that ζ is of odd multiplicative order and therefore any power of ζ is a square in $\mathbb{Z}[\zeta]$. Using (4.10) we conclude that $\det C = -a\delta^2$, where $\delta \in (\mathbb{Z}[\zeta])^*$. Since $\det C$ is an integer and a is a non-zero integer or half-integer, we have that $\delta^2 \in \mathbb{Q}$. Hence, $\delta^2 \in \mathbb{Z}^*$, i.e., $\delta^2 = \pm 1$. On the other hand, $\mathbb{Q}(\zeta)$ does not contain primitive fourth roots of 1, since $[\mathbb{Q}(\zeta, \sqrt[4]{1}) : \mathbb{Q}] = [\mathbb{Q}(\zeta \cdot \sqrt[4]{1}) : \mathbb{Q}] = 2(p-1)$ and $[\mathbb{Q}(\zeta) : \mathbb{Q}] = p-1$. Therefore, $\delta^2 = 1$. This completes the proof. \square

Proof of Corollary 1. Since $\varepsilon > 1$, we have immediately that $a > 0$. Hence, $\det C < 0$.

Now write $\varepsilon^h = (\alpha + \beta\sqrt{p})/2$, where α and β are integers. Since ε^h is a quadratic unit of norm -1 (see [10, Ch. 4, §18.4] or [4, Ch. 5, Sec. 4, Ex. 5]), we have

$$(4.11) \quad \alpha^2 - p\beta^2 = -4.$$

Consider (4.11) modulo 16. A direct search shows that

- for $p \equiv 1, 9 \pmod{16}$, $\alpha \equiv 0, 4, 8, \text{ or } 12 \pmod{16}$, i.e., $a = \alpha/2$ is even;
- for $p \equiv 5, 13 \pmod{16}$, $\alpha^3 + 3\alpha\beta^2p \equiv 0 \pmod{16}$. In particular, raising ε^h to the third power, we have that $a = (\alpha^3 + 3\alpha\beta^2p)/8$ is even.

\square

Acknowledgements

The author is grateful to J. Sondow and T. Amdeberhan for commenting an earlier version of the paper.

References

- [1] *The On-line Encyclopedia of Integer Sequences*, <http://oeis.org/>
- [2] *Research Problems [BCC20]*, Discrete Mathematics, 308 (2008), no. 5-6, 621–630.
- [3] T. Amdeberhan and D. Zeilberger, “*Trivializing*” *Generalizations of some Izergin–Korepin-type determinants*, Discrete Math. Theor. Comp. Sci. 9 (2007), no. 1, 203–206.
- [4] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, New York, 1966.

- [5] A. L. Cauchy, *Mémoire sur les fonctions alternées et sur les sommes alternées*, Exercices d'Analyse et de Phys. Math. 2 (1841), 151–159. (= *Oeuvres*, ser. 2, vol. 12, 173–182)
- [6] R. Chapman, *Determinants of Legendre symbol matrices*, Acta Arith. 115 (2004), 231–244.
- [7] R. Chapman, *Steinitz classes of unimodular lattices*, European J. Combin. 25 (2004), 487–493.
- [8] R. Chapman, *My evil determinant problem*, Unpublished note (2009), <http://secamlocal.ex.ac.uk/people/staff/rjchapma/etc/evildet.pdf>
- [9] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd edition. Springer, 1990.
- [10] H. Hasse, *Vorlesungen über Zahlentheorie*, Springer, Berlin, 1950.
- [11] R. Stanley, *Enumerative combinatorics*, vol. 2. Cambridge University Press, 2001.
- [12] M. Vsemirnov, *On the evaluation of R. Chapman's "evil determinant"*, Lin. Alg. Appl. 436 (2012), 4101–4106.